SPAWAR

News Release

United States Navy
Space and Naval Warfare Systems Command
Public Affairs and Corporate Communications
4301 Pacific Highway, San Diego CA 92110-3127
Telephone: 619-524-3432 FAX: 619-524-3469

Release Nr. NR-2001-016
Friday, July 20, 2001

NMCI Update for July 18, 2001 - The rest of the story.

By Scott Randall
Director, SPAWAR PD-16
Deputy Director, PEO-IT

The following is an email sent by Mr. Scott Randall, Director SPAWAR PD-16 / West Coast Deputy Director PEO-IT, sent to all SPAWARSYSCOM personnel:

Many of you may have seen recent stories suggesting a significant slip in the NMCI schedule and the potential for adverse actions, even potential termination, of the contract. As we all know, these types of accusations make good headlines and fuel newspaper sales. I'd like to address some of those issues in greater detail and provide some insight into the probable outcomes. As Paul Harvey would say, here is "...the rest of the story".

First, lets talk about the issue of the contract having slipped up to a year from proposed schedules.

The contract was originally intended for award last summer but was held up for a variety of reasons until October 6th. This type of service contract was the first of its kind and has set a model for future acquisition. But like any "first", it sometimes takes a little longer to explain a new process. Once the contract award was made, the brand new Information Strike Force (ISF) was faced with the daunting task of getting "seats" on line as quickly as possible while simultaneously meeting changing test requirements.

The Information Strike Force has done extremely well taking over the “as is” environment and management of the existing information technology networks, hardware and software. From a "standing start" they have more than 40,000 “seats” under their management (this is close to the limit for the pre-test orders that is allowed by Congress). The ISF has stood up two Network Operations Centers and Help Desk Centers, and they are moving forward to "cutting over" the seats they are managing to the new network and with new computers. NMCI has begun an extremely difficult task, it is bringing the new nationwide network on line while simultaneously implementing a level of security management we have never experienced before. The industry team has done all this in the space of six months and has exceeded our expectations.

The very aggressive schedule that was jointly set between the Navy's Program Management Office (SPAWAR PMW-164) and the Information Strike Force shortly after award of the contract has been maintained with only minimal slippage (weeks versus the year reported in some news articles). The ISF is currently hiring staff and preparing to execute the full level of orders that the Navy intends to place next year.

The second issue raised in recent news articles is a concern about what procedures will be used to test the Navy Marine Corps Intranet. We are all concerned about the difficult challenge of adapting commercial best practices into a military testing, evaluation and acquisition process.

From the outset, this initiative was designed as a commercial procurement and the intent was to leverage industry’s leading edge best practices in most areas — including testing. While it was recognized that this is a military network subject to stringent Information Assurance requirements, those requirements were “built in” the planned test and certification processes.

What was not anticipated was the perception that NMCI should undergo full military Operational Testing like that applied to weapon systems. This level of testing is very formal and comes with its own requirements which are much more detailed and stringent than those of commercial best practices. If it is decided that NMCI must complete this weapons system level of testing prior to accepting more orders or providing more services, this will understandably add to the original timetable for implementation.

While the final decision on testing levels and schedules has not been reached, it is likely there will be a compromise that accommodates the need for “more than sufficient” testing while also allowing the program to proceed at the reasonable pace needed by our Sailors and Marines. We hope the final decision will be a "phased" test approach to ensure that program goals are being met at various “checkpoints,” while still continuing to field this increased capability to the Fleet.

Major hurdles must still be overcome

A real concern to the NMCI government and industry team is the number of legacy computer applications that we are finding across the Navy. At the beginning of this effort, we as a Navy had no idea how many different applications were in use and the incredible support required to maintain them all. We are already into the tens of thousands of applications with only a fraction of the Navy having been surveyed.

Each of those separate applications has to be evaluated, tested, and certified against a variety of requirements, not the least of which is the security requirements. Applications that are non-compliant with Navy policies need to be taken out of service or have to have a work-around developed and certified before it can be included in the NMCI certified software set. This is a very rigorous and time-consuming process and is indeed one of the most significant objectives to be overcome as we make the transition to a common operating system and common operating environment.

Here at SPAWAR, as well as elsewhere in the Navy, we are working hard to reduce the number of applications that will transition to the NMCI. So far we have identified 3,955 applications and have eliminated 1,915. This effort results in a huge savings in logistics and software support in addition to the value provided by the contract alone, and will significantly increase our ability to collaborate using common sets of software. The issue of legacy applications is highlighted by the implementation of NMCI, but is truly a Navy-wide concern that is also being addressed by the Task Force Web efforts.

In summary, the NMCI is alive and well and is making tremendous progress against a very challenging task. This is the first initiative of this kind or scope and many of the processes and procedures to execute the contract are still being developed. These processes are being discussed, reviewed and established by many stakeholders of the NMCI — customers, DoN CIO, CNO, the PMO and the PEO-IT.

The Navy has tremendous benefits to gain through this contract. We will gain a high performance network, built-in refresh for hardware and software, and a vastly improved Information Assurance practice. We have not identified any showstoppers that would make the business case less attractive. The bottom line is that we will continue to press on, address and resolve the issues as they arise, and make this program a success story for the Navy and for the Defense Department.

- # -